



Payrix

Client Data Encryptor

User guide

Last updated 28 September 2021

Australia: 1300 592 283 | admin@Payrix.com.au
New Zealand: 0800 480 054 | admin@Payrix.com.au
USA: 844-517-5981 | admin@Payrix.com.au

www.Payrix.com/au (AU)
www.Payrix.co.nz (NZ)
www.Payrix.com (USA)

INTRODUCTION

Payrix is compliant with the Payment Card Industry Data Security Standard (PCI DSS) Level 1 – this is the highest level of compliance for the industry’s mandate on secure storage, processing and transmission of data. We have an obligation to protect cardholder data and prevent its unauthorised use.

There may be instances when data needs to be transferred between Payrix and a third-party such as another payment service provider. To ensure this process is PCI DSS compliant, data can be encrypted with public and private keys generated using Payrix's Client Data Encryptor.

Payrix can encrypt data and upload it to a secure file sharing service. A third-party can then download and decrypt the data.

At Payrix, only authorised staff can access data during the data transfer process.

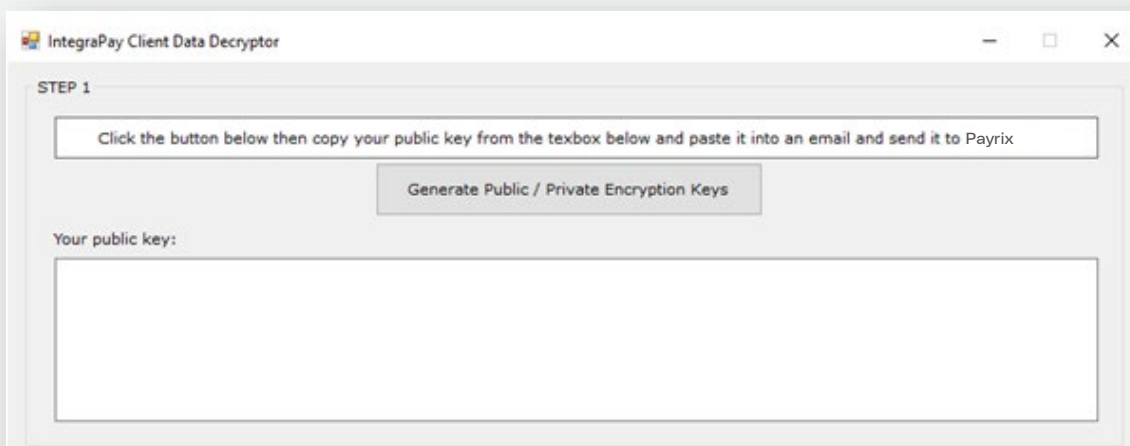
STEPS TO TAKE

The steps below are for a payment service provider to follow.

- Payrix will have already provided you with the Client Data Encryptor application file – Payrix.ClientDataDecryptor.exe
If you haven't received this file you should [contact our Client Support team](#)
- Save the file on to your own computer or server, and run the application.
- Terms and conditions will be displayed – agree to these before proceeding.
- Instructions are then displayed for the two steps you need to take.

Step 1: Generating an encryption key

- Under the **Step 1** area of the display, click the button **Generate Public / Private Encryption Keys**.
- The encryption key will appear in the box.
- Copy the encryption key and paste it into an email, and send it to your contact at Payrix.

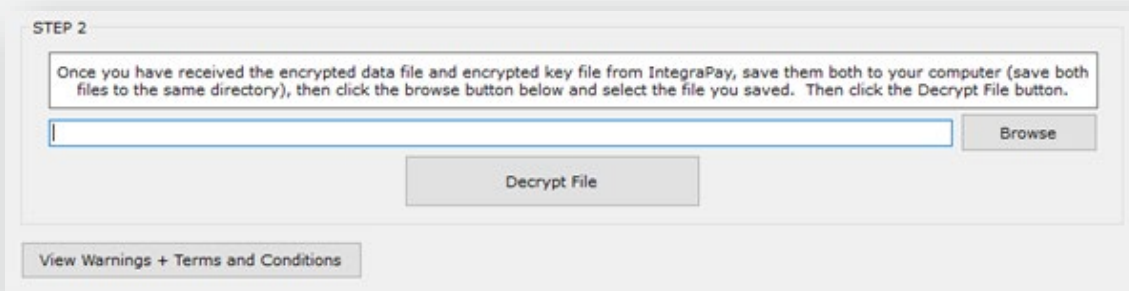


- Payrix will then encrypt the data with this key, and upload it to its secure location at box.com – or to an agreed alternative location.

STEPS TO TAKE

Step 2: Download and decrypt the data

- Payrix will email you a link to box.com when the data is ready to download.
- Download two files, and save them on your computer or server:
 - Encrypted data file
 - Associated encryption key file
- Return to the Client Data Encryptor.
- Under the **Step 2** area of the display, click **Browse**.
- Locate the encrypted data file that you saved earlier, click **OK**.
- Click **Decrypt File** – the data file will then be decrypted for you.



The screenshot shows a web interface for Step 2. At the top, it says "STEP 2". Below that is a text box with instructions: "Once you have received the encrypted data file and encrypted key file from IntegraPay, save them both to your computer (save both files to the same directory), then click the browse button below and select the file you saved. Then click the Decrypt File button." Below the text box is a file selection input field with a "Browse" button to its right. Below the input field is a "Decrypt File" button. At the bottom left, there is a button labeled "View Warnings + Terms and Conditions".

HELP AND SUPPORT

If you require further assistance, please contact Payrix Client Support:

Australia

Ph: 1300 592 283

Email: admin@Payrix.com.au

USA

Ph: 844-517-5981

Email: admin@Payrix.com.au

New Zealand

Ph: 0800 480 054

Email: admin@Payrix.com.au